REMARKS

Claims 1-32 are pending in the present application

This Amendment is in response to the Office Action mailed March 4, 2009. In the Office Action, the Examiner rejected claims 1-14, 10-13, 18-23, 27, and 28 under 35 U.S.C. §102(b) and claims 15-17, 24-26 and 29-32 under 35 U.S.C. §103(a). Reconsideration in light of the remarks made herein is respectfully requested.

On November 30, 2007, the undersigned attorney conducted a telephone conference and discussed what elements of U.S. Patent No. 6,289,455 (Kocher) were construed as the "first value", the "second value" and the "third value" as set forth in claims 1 and 14. The Examiner identified that the "rights key", "KDM" and "CDK" were interpreted by him to constitute the "first value", the "second value" and the "third value," respectively.

Formal Request for Examiner's Interview

Applicant respectfully requests the Examiner to contact the undersigned attorney to discuss the allowability of the pending claims especially if, after his review, there are still outstanding rejections regarding patentability. The undersigned attorney can be reached at the telephone number listed below.

Rejection Under 35 U.S.C. § 102

Claims 1-14, 18-23, 27 and 28 were rejected under 35 U.S.C. §102(b) as being anticipated by Kocher (Patent No. 6,289,455). Applicant respectfully requests the Examiner to withdraw this rejection because a *prima facie* case of anticipation has not been established.

As the Examiner is aware, to anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Vergegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the…claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989). Herein, all of the claim limitations are not found in Kocher.

A. Claim 1

For instance, with respect to claim 1, the Office Action does not clearly identify the elements set forth in the claims. However, based on the Examiner's interview conducted on November 30, 2007, the undersigned attorney conducted a telephone conference and discussed what elements of U.S. Patent No. 6,289,455 (Kocher) were construed as the "first value", the "second value" and the "third value" as set forth in claims 1 and 14. The Examiner identified that the "rights key", "KDM" and "CDK" were interpreted by him to constitute the "first value", the "second value" and the "third value," respectively.

Applicant respectfully disagrees that the "rights key", "KDM" and "CDK" disclose the "first value", the "second value" and the "third value," respectively, as delineated in claim 1.

Claim 1 recites, among other things, "a control word key ladder logic to produce (i) a first value generated based on a conditional access (CA) random value and the unique key, (ii) a second value generated using the first value, and (iii) a third value recovered by a cryptographic operation using the second value; a first cryptographic unit to descramble incoming content in a scrambled format based on the third value; and a second cryptographic unit to decrypt incoming encrypted data using the first value."

As described at column 11, lines 40-63 of Kocher, the interface control processor (ICP) uses the key derivative message (KDM) to obtain a content decryption key (CDK) generator value. The CDK generator value may be an encrypted form of the CDK and the CDK generator value is part of the KDM. The KDM can identify whether the rights key is appropriate for processing each CDK generator (Kocher, col. 11, lines 40-63). The CDK generator is transformed by the rights key using pseudo-asymmetric function F_3 to produce a F_3 result and the ICP produces the final CDK from the F_3 result (Kocher, col. 11, lines 53-63).

Accordingly, the KDM is generated before the rights key is involved in transforming the CDK generator into the F_3 result from which the final CDK is produced. The invention in Kocher is illustrated below:

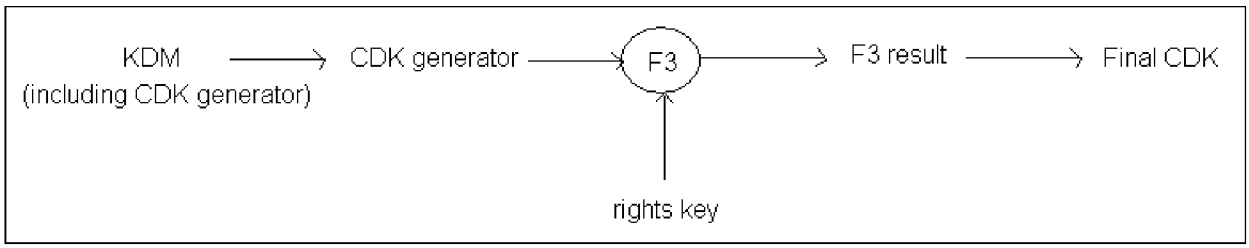

Figure A: Kocher's invention

Therefore, *the KDM (second value) is not generated using the rights key (first value). Emphasis added.* Instead, the KDM is generated before the rights key operates on the CDK generator.

Additionally, the Examiner alleges that "the rights keys *[first value]* are used to derive the CDK's which are part of the KDM *[second value]*" (Final Office Action, page 8) such that the rights keys are thus used to generate the KDM (Final Office Action, page 8). Applicant respectfully disagrees and submits that the Examiner's argument is illustrated below:

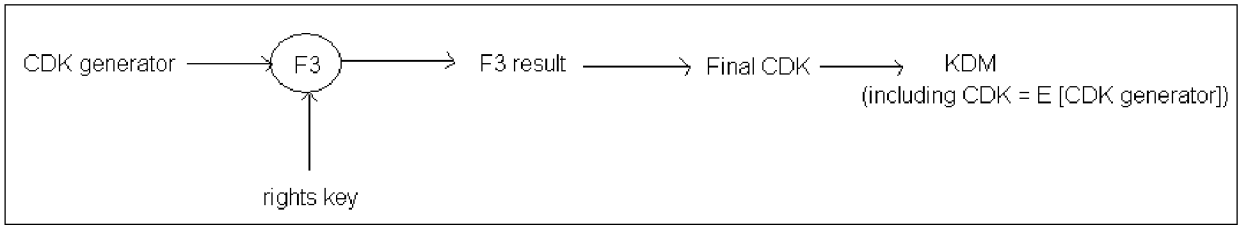

Figure B: Examiner's argument

Applicant respectfully submits that the Examiner misconstrues the teachings of Kocher. As discussed above, Kocher discloses the KDM being generated before the rights key is involved. Accordingly, Applicant respectfully submits that it is inconsistent with the teachings of Kocher to conclude that "KDM is generated using the rights key" merely because the KDM includes the CDK generator value from which the final CDK is derived using the rights keys. Therefore, Kocher fails to describes control word key ladder logic to provide a second value, allegedly KDM, generated using the first value, allegedly the rights key.

In the response to argument section of the Office Action, the Examiner states:

> "with respect to the Applicant's argument that "it is false to conclude that the KDM is generated using the rights key merely because it includes the CDK

> generator from which the CDK is derived," Applicant is directed to Kocher, column 11, lines 40-63. As described above, Kocher discloses the rights keys (i.e., first derivative keys) are used to derive the CDK's which are a part of the KDM (i.e., mating key). Therefore, Kocher discloses the first derivative ke is used to generate a mating key." (Office Action, page 10)

Applicant respectfully submits that the Examiner merely repeats the rejection without taking note of and answering the substance of Applicant's arguments.

> Where a claim is refused for any reason relating to the merits thereof it should be "rejected" and the ground of rejection fully and clearly stated. See MPEP § 707.07(d). Where the applicant traverses an objection, the Examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it. See MPEP § 707.07(f).

Specifically, Applicant has delineated above that the cited portion of Kocher merely discloses that the CDK generator is an encrypted form of the CDK and is part of the KDM (Kocher, col. 11, lines 41-43). Using the rights key, the CDK generator is transformed to produce the F_3 result which is subsequently used to produce the final CDK (Kocher, col. 11, lines 40-63). See Figure A above. Therefore, the KDM is generated before the rights key is involved in transforming the CDK generator, and thus, the KDM cannot be generated using the rights key.

Additionally, claim 1 includes the limitation of "a second cryptographic unit to decrypt incoming encrypted data using a first value." The Examiner alleges that the "first value" is the rights key. Per Kocher, the "rights key" is a derivation of the content identifier for use in post-payment processing (Kocher, col. 11, lines 6-23). The rights key, however, is not used for decryption of incoming encrypted data.

In the "Response to Arguments" section of the Office Action, the Examiner alleges:

> "Kocher further discloses the rights key includes a content identifier. Therefore, it is reasonable to read that the first derivative key (i.e., the rights key) would be used to generate the mating key (i.e., KDM)" (Office Action, page 10).

Applicant respectfully disagrees. Again, Applicant respectfully submits that Kocher teaches that the rights key is a derivation of the content identifier (Kocher, col. 11, lines 6-23) and the CDK generator is part of the KDM (Kocher, col. 11, lines 41-43). However, since the KDM is generated before the rights key is involved in the transformation of the CDK generator,

one cannot reasonably conclude that the rights key, which is used for post-payment processing in Kocher, would be used to generate the KDM, which the Examiner now alleges to be the mating key.

Hence, Applicant respectfully submits that claim 1 is in condition for allowance.

B. Claim 13

Similarly, with respect to claim 13, the Examiner has advised the undersigned attorney that he has construed the "rights key", "KDM" and "CDK" as the "first value", "second value" and "third value," respectively.

Applicant incorporates by reference the arguments set forth above. Specifically, as above, the KDM, allegedly the second value, is not recovered from a mating key generator… using the rights key, allegedly first value, because the KDM is generated before the rights key is involved in the transformation of the CDK generator value.

Additionally, claim 13 recites, among other things, "a second value recovered from a mating key generator undergoing a cryptographic operation using the first value where the mating key generator is a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number." *Emphasis Added.*

Applicant further traverses the rejection because a second value, allegedly KDM, is not recovered from a mating key generator undergoing a cryptographic operation using the first value, allegedly the rights key. Kocher merely teaches that KDM is "a message generated by a content provider... KDMs are usually transmitted with…corresponding content" (Kocher, col. 8, lines 17-20). The ICP receives a KDM from the playback device (Kocher, col. 11, lines 38-40; Figure 5).

Therefore, since the KDM is merely generated by a content provider and received from the playback device, there is no teaching or suggestion that the KDM is recovered from a mating key generator, let alone, a mating key generator which "is a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number" as delineated in the claim.

In the "Response to Arguments" section of the Office Action, the Examiner maintains the allegations that Kocher, column 8, lines 17-20 and column 11, lines 38-40 and figure 5 disclose

the elements of claim 13. As discussed above, Applicant respectfully disagrees and submits that Kocher does not disclose "a second value [allegedly KDM] recovered from a mating key generator undergoing a cryptographic operation using the first value [allegedly the rights key]" because the KDM is generated before the rights key is involved in the transformation of the CDK generator.

Moreover, the Examiner states that:

> "the REM (Rights enablement message) includes the rights key including an identifier of content… Kocher, column 11, lines 13-18, explicitly disclose: "The content identifier can be a simple identifier, a randomly produced or cryptographically generated value, a counter, a combination of parameters, etc… and may be generated by the content provider, ICP, playback device, CryptoFirewall, etc…" Therefore, the mating key generator is a message that comprises at least one of a set-top box manufacturer identifier, a service provider identifier, a CA provider identifier, and a mating key sequence number" (Office Action, page 10-11).

Thus, the Examiner alleges that the REM is the mating key generator. Applicant respectfully disagrees and submits that even assuming that the REM includes the rights key that is derived from the content identifier, there is no teaching that the KDM, allegedly the second value, is recovered from the REM, allegedly a mating key generator.

Please note that a rights key being derived from the content identifier is not the same as the rights key including the content identifier. Here, the rights key is derived from the content identifier (Kocher, col. 11, lines 6-23).

Even assuming that the REM corresponds to the mating key generator which includes the content identifier, nothing in the content identifier corresponds to "at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number." In fact, the Examiner's cited portion of Kocher merely states that "the content identifier can be a simple identifier, a randomly produced or cryptographically generated value, a counter, a combination of parameters, etc…"

Additionally, Kocher states "the content identifier may be generated by the content provider, ICP, playback device, CryptoFirewall." Even if the content identifier is generated by the content provider, it is a leap of logic to conclude that the content identifier then includes the content identifier includes "at least one of a set-top-box manufacturer identifier, a service

provider identifier, a conditional access (CA) provider identifier and a mating key sequence number…", as recited in the claim.

Hence, Applicant respectfully submits that claim 13 is in condition for allowance.

C. Claim 22

With respect to independent claim 22, the Examiner appears to have construed the "rights key", "KDM" and "CDK" as the "first derivative key", "mating key" and the "control word," respectively. Applicant respectfully traverses the rejection because claim 22 includes at least two claim limitations that are not taught by Kocher, namely:

> "a second process block configured to generate a mating key from a mating key generator using the first derivative key, the mating key generator being a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number, and
>
> a third process block configured to recover a control word by decrypting an encrypted control word using the mating key."

As claimed, Applicant respectfully disagrees that the second process block, namely the process to access content as described on column 11 (lines 35-45) of Kocher, is configured to generate a mating key (KDM) from a mating key generator (CDK generator) using the first derivative key (rights key).

As discussed above, the rights key has no involvement in the generation of the KDM. The Examiner alleges that "the rights keys (i.e. first derivative keys) are used to derive the CDKs which are part of the KDM (i.e. mating key). Therefore, Kocher discloses the first derivative key is used to generate a mating key" (Office Action, page 9). Applicant respectfully disagrees. As above, while the final CDK is derived using the rights keys, Applicant respectfully submits that KDM is generated before the rights key is involved in the transformation of the CDK generator value. Thus, the Examiner's conclusion that the KDM is generated using the rights key is contrary to the teachings of Kocher.

Moreover, as discussed above, the KDM is merely generated by a content provider and received from the playback device. There is no teaching or suggestion that the KDM is generated from a mating key generator, previously alleged to be the CDK generator, using the rights key (i.e., the first derivative key).

The Examiner alleges that "Kocher further discloses the rights key includes a content identifier" (Final Office Action, page 8). As discussed above, since the KDM is not generated using the rights key, even if the rights key was to include a content identifier, the rights key cannot correspond to the mating key generator, as delineated in the claim.

Furthermore, the claim recites "to generate a mating key from a mating key generator using the first derivative key" such that the mating key generator and the first derivative key are separate and distinct elements in the claim. Given that the Examiner alleges that the rights key corresponds to the first derivative keys as well as the mating key generator, Kocher fails to disclose these elements of the claim.

In addition, Kocher does not describe a third process block configured to recover a control word, allegedly the CDK, by decrypting an encrypted control word using the mating key, allegedly the KDM. The KDM does not appear to be used for any decryption operations (Kocher, col. 11, lines 33-65; Figure 5).

The Examiner alleges that "the KDM (i.e. mating key) is used to identify the rights key, which is then used to transform the CDK and decrypt the content (i.e. decrypt the control word)" (Office Action, page 10). Applicant respectfully disagrees.

Applicant respectfully submits Kocher merely discloses using the CDK to decrypt the content (Kocher, col. 11, lines 64-65; Figure 5). Accordingly, the CDK is used to decrypt the content and not the KDM, as alleged by the Examiner.

Furthermore, the content in Kocher is merely digital content is "a digital representation of human-interpretable material, such as pictures, audio tracks, video segment text" (Kocher, col. 8, lines 1-6). In contrast, a control word is used for descrambling scrambled content (See Specification, page 38, for further details). Thus, the digital content in Kocher cannot be a control word, as alleged by the Examiner.

In the response to argument section of the Office Action, the Examiner merely reiterates his arguments which have been addressed by Applicant. Applicant respectfully submits that as above, the Examiner fails to answer the substance of Applicant's arguments.

Hence, Applicant respectfully submits that claim 22 is in condition for allowance.

D. Claim 28

With respect to claim 28, similar to the arguments presented above, Kocher does not describe the recovery of the plurality of control words (CDKs) using the plurality of mating keys (KDMs). Applicant incorporates the arguments made above and respectfully requests the Examiner to withdraw the rejection or to provide ample evidence in support of the rejection. Withdrawal of the outstanding §102(b) rejection is respectfully requested.

E. Claims 2-12, 14, 18-21, 23 and 27

With respect to claims 2-12, 14, 18-21, 23 and 27, Applicant respectfully traverses the outstanding §102(b) rejection because a *prima facie* case of anticipation has not been established for these claims. Based on the dependency of the above-identified claims on independent claims 1, 13 and 22, which are believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traversing the rejection is necessary. For illustrative purposes, however, we shall discuss a few of these claims to illustrate that Kocher clearly does not anticipate these claims.

In light of the foregoing, Applicant respectfully requests that the Examiner withdraw the outstanding §102(b) rejection.

Rejection Under 35 U.S.C. § 103

Claims 26 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

To establish a *prima facie* case of obviousness, certain basic criteria must be met. For instance, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. MPEP §2143. Applicant respectfully submits that the combined teachings do

not address each and every limitation, and thus no *prima facie* case of obviousness has been established.

Furthermore, the Supreme Court in Graham v. John Deere, 383 U.S. 1, 148 USPQ 459 (1966), stated: "Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined." MPEP 2141. In KSR International Co. vs. Teleflex, Inc., 127 S.Ct. 1727 (2007) (Kennedy, J.), the Court explained that "[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order *to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue*." *Emphasis Added.* The Court further required that an explicit analysis for this reason must be made. "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." KSR, 127 S.Ct. at 1741, quoting In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006). In the instant case, Applicant respectfully submits that there are significant differences between the cited references and the claimed invention and there is no apparent reason to combine the known elements in the manner as claimed, and thus no *prima facie* case of obviousness has been established.

Herein, Kocher does not teach or suggest all of the claim limitations and incorporates the arguments set forth above. Withdrawal of the outstanding §103 rejection is respectfully requested.

Furthermore, claims 15-17, 24, 25 and 30-32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher in view of Wasilewski (U.S. Patent Publication No. 2004/003008). Herein, Applicant respectfully submits that neither Kocher nor Wasilewski, alone or in combination, describe or suggest all of the claim limitations set forth in these claims, especially those limitations denoted above in traversing the outstanding §102(b) rejection. Applicant incorporates these arguments by reference. Also, based on the dependency of the above-identified claims on independent claims 1, 13, 22 and 28, which are believed by Applicant

to be in condition for allowance, no further discussion as to the grounds for traversing the rejection is necessary.

Applicant respectfully requests that the Examiner withdraw the rejection of claims 15-17, 24, 25 and 30-32 under 35 U.S.C. § 103(a) as being unpatentable over the combined teachings of Kocher and Wasilewski.

Conclusion

Applicant respectfully requests that the corrected claims with amended claim identifiers be accepted and entered.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: June 4, 2009

By / William W. Schaal /

William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)